

## 明細書

### 発明の名称

通信プロトコルの試験系列生成方法および装置

### 発明の背景

#### 1. 発明の属する技術分野

本発明は、試験系列生成技術に関する。本発明は、特に、通信プロトコルの試験系列生成問題をSAT問題へ変換し、変換後のSAT問題を解くことにより通信プロトコルの試験系列を生成する通信プロトコルの試験系列生成方法および装置に関する。

#### 2. 関連技術の説明

SAT問題(Satisfiability problem)は典型的なNP完全問題として知られ、学術的によく研究されている組合せ最適化問題である。SAT問題では、与えられた和積形論理式  $f$  に対して、充足可能性の判定や充足可能な場合に  $f$  中の変数に対する真理値割当をできるだけ高速に算出することが要求される。近年、SATアルゴリズムの性能が改善され、Electronic Design Automation の分野などにおいて実用的な問題へ適用されている。

有限状態機械(FSM: Finite State Machine)でモデル化した通信プロトコルに対して試験を行う場合には、FSMの状態を識別する入出力系列が使われる。このような系列としてDS(Distinguish Sequence)やUIO系列(Unique Input/Output Sequence)などがある。

これらの系列は、FSMのある1つの状態でのみ実行できる入出力系列である。一般に任意のFSMの各状態についてDSやUIO系列が存在するとは限らない。しかしUIO系列については、実際に使われるプロトコルを表したFSMで、ほとんどの場合に存在することが知られている。また、一般に各状態に対して複数のUIO系列が存在する場合もある。

F S Mでモデル化される通信プロトコルに対して試験を行う場合は、プロトコル仕様に記述されている状態および状態遷移が実装に存在するのか、また正しく実装されているのかを確認する。プロトコル仕様に記述されている状態が実装に存在するのかを確認する試験系列を作成する問題、状態遷移が正しく実装されているのかを試験する試験系列を作成する問題が試験系列生成問題である。

実装にある状態  $s$  が存在するかを確認するには、F S Mを初期状態から状態  $s$  へ遷移させる入出力系列（先行系列）のあとに、状態  $s$  に対するU I O系列を接続した系列を実装に対して適用すればよい。

また、状態  $s$  から状態  $s'$  への状態遷移  $t$  を確認するには、F S Mを初期状態から状態  $s$  へ遷移させる先行系列のあとに、状態遷移  $t$  に対応する入出力と状態  $s'$  に対するU I O系列を接続した系列（部分系列）を実装に対して適用すればよい。すべての状態および状態遷移に対して上記の入出力系列（部分試験系列：先行系列+U I O系列または先行系列+部分系列）を生成、接続することで試験系列を生成する。

ある部分試験系列の先行系列として、別の部分試験系列を使うことによって試験系列を短くすることができる。また、各状態に対して複数のU I O系列が存在する場合があるため、U I O系列の選択によって試験系列の長さが変化する。さらに、U I O系列や部分系列が共通部分を持っている場合、それらを重複させることでより短い試験系列を生成することができる。

一般に、系列の重複を考慮しない場合に最適な試験系列を生成する問題はNP完全問題であることが知られている。また、系列の重複を考慮した場合もNP完全問題であることが知られている。

従来の試験系列生成手法として、F S Mの各状態に対してU I O系列を生成するアルゴリズムと状態および状態遷移を確認する試験系列生成手法がある。また、F S Mの各状態に自己ループがあるような場合、または各状態から初期状態への遷移（リセット遷移）がある場合に、状態遷移を確認する最適な試験系列を効率良く解くアルゴリズムがある。

また、従来の試験系列生成手法として、各状態に対してU I O系列を1つ選び、部分系列の重複を考慮しない試験系列を生成する手法や、複数のU I O系列を考慮して状態遷移を確認する試験系列を生成する手法がある。

しかし、上記従来の技術では、U I O系列に重複がある場合に状態の存在を確認する試験系列を作成したり、部分系列に重複がある場合に状態遷移が正しく実装されているかを試験する試験系列を生成すると、試験系列長が長くなったり、試験系列生成処理の実行時間が長くなったりするという問題が生じる。

#### 発明のサマリー

本発明は、通信プロトコルの仕様を示すF S M、F S Mの各状態に対するU I O系列、確認したい状態、制約条件、最大試験系列長を入力するステップと、通信プロトコルの試験系列生成問題をS A T問題に変換するステップと、既存のS A T問題を解決するソフトウェアであるS A T s o l v e rを用いてS A T問題を解いて、試験系列を生成するステップとを実行することにより、プロトコル仕様に記述されている状態が実装に存在するのを確認する試験系列を生成する。

上記通信プロトコルの試験系列生成問題をS A T問題に変換するステップでは、F S Mを修正するステップと、修正後のF S Mに基づいて試験系列生成問題を和積形論理式の節で表現するステップとを実行する。

また、本発明は、通信プロトコルの仕様を示すF S M、F S Mの各状態に対するU I O系列、試験したい状態遷移、順序制約、時間制約、最大試験系列長を入力するステップと、通信プロトコルの試験系列生成問題をS A T問題に変換するステップと、既存のS A T s o l v e rを用いてS A T問題を解いて、試験系列を生成するステップとを実行することにより、プロトコル仕様に記述されている状態遷移が正しく実装されているかを試験する試験系列を生成する。

上記通信プロトコルの試験系列生成問題をS A T問題に変換するステップでは、F S M

を修正するステップと、修正後のF S Mに基づいて試験系列生成問題を和積形論理式の節で表現するステップとを実行する。

#### 図面の簡単な説明

F i g. 1 は、本発明の試験系列生成装置の構成例を示す図である。

F i g. 2 は、試験系列生成問題変換部の構成を示す図である。

F i g. 3 は、F S Mで記述したプロトコル機械の例を示す図である。

F i g. 4 は、U I O系列を示す図である。

F i g. 5 は、試験系列生成処理フローの例を示す図である。

F i g. 6 は、H'、I'を構成するアルゴリズムを示す図である。

F i g. 7 は、修正後のF S Mを示す図である。

F i g. 8 A は、F S Mを示す図である。

F i g. 8 B は、修正後のF S Mを示す図である。

F i g. 9 A は、F S Mを示す図である。

F i g. 9 B は、修正後のF S Mを示す図である。

F i g. 10 は、D H C Pの動作を示すF S Mを示す図である。

F i g. 11 は、本発明の実施例1の試験系列生成方法の適用例を示す図である。

F i g. 12 は、本発明の実施例1の試験系列生成方法の適用例を示す図である。

F i g. 13 は、F S Mを示す図である。

F i g. 14 は、U I O系列を示す図である。

F i g. 15 は、試験系列生成処理フローの例を示す図である。

F i g. 16 は、修正後のF S Mを示す図である。

F i g. 17 は、本発明の実施例2の試験系列生成方法の適用結果を示す図である。

F i g. 18 は、本発明の実施例2の試験系列生成方法の適用結果を示す図である。

F i g. 19 は、本発明の実施例2の試験系列生成方法の適用結果を示す図である。

Fig. 20は、本発明の実施例2の試験系列生成方法の適用結果を示す図である。

#### 好適具体例の詳細な説明

本発明では、有限状態機械（FSM：Finite State Machine）でモデル化される通信プロトコルに対してSATを用いた適合性試験系列生成手法を提案する。

Fig. 1は、本発明の試験系列生成装置の構成例を示す図である。Fig. 1において、1は通信プロトコルの試験系列を生成する試験系列生成装置、11は通信プロトコルの仕様を示すFSMと確認したい状態等またはFSMと試験したい状態遷移等を入力する仕様入力部、12は通信プロトコルの試験系列生成問題をSAT問題へ変換する試験系列生成問題変換部、13は変換後のSAT問題を解いて試験系列を生成する試験系列生成部である。

Fig. 2は試験系列生成問題変換部の構成を示す図である。Fig. 2において、121はFSMを修正するFSM修正部、122は修正後のFSMに基づいて試験系列生成問題を和積形論理式の節で表現する和積形論理式定式化部である。

#### （実施例1）

本発明の実施例1では、UIO系列を利用して、プロトコル仕様に記述されている状態が実装に存在するのかを確認する試験系列を生成する。具体的には、本発明の実施例1では、SATアルゴリズムを用いて、複数のUIO系列およびUIO系列の重複を考慮して、状態確認を行う最適な試験系列を生成する手法を提案する。

本発明の実施例1における提案手法は、FSMの動作や試験系列に対する条件を論理式で記述する。本発明の実施例1の提案手法の有用性を評価するため、後述するように、本発明の実施例1の提案手法に基づいて試験系列生成プログラムを実装し、DHCP (Dynamic Host Configuration Protocol)に適用した。

まず、本発明の実施例1の説明の前提として、通信プロトコルの仕様を示すプロトコル機械、適合性試験、SAT問題について説明する。

### (プロトコル機械)

プロトコル機械は、Mealy型決定性有限状態機械(FSM)とし、5字組( $S, X, Y, H, s_0$ )で定義する。ここで、 $S, X, Y$ はそれぞれ状態の有限集合、入力記号の有限集合、出力記号の有限集合を表す。

また、 $H$ は状態遷移( $u, v, x, y$ )の有限集合を表す。ただし、 $u, v \in S$ は始状態、終状態、 $x \in X$ は入力、 $y \in Y$ は出力を表す。実施例1においては、 $s_0$ は初期状態を表す。Fig. 3にFSMで記述したプロトコル機械の例を示す。

### (適合性試験)

本発明の実施例1では、プロトコル機械の実装(IUT: Implementation Under Test)に対して、プロトコル機械の各状態が正しく実装されているかを確認する試験系列を生成する。

IUTに対してある状態 $s$ を確認したい場合は、プロトコル機械が初期状態から状態 $s$ へ遷移する入力系列(先行系列)をプロトコル仕様から生成し、その系列をIUTに与えた後、IUTが状態 $s$ であるかどうかを確認すればよい。このため、FSMの各状態を識別する必要がある。

FSMの各状態を識別する系列としてUIO系列(Unique Input/Output sequence)がある。FSM  $M$ の状態 $s$ に対するUIO系列とは、FSM  $M$ において状態 $s$ 以外のどの状態からも実行することができない入出力系列のことである。

ここで、入出力系列 $\alpha = (i_1/o_1)(i_2/o_2)\cdots(i_m/o_m)$  ( $i_j$ :入力、 $o_j$ :出力,  $1 \leq j \leq m$ )がFSM  $M$ の状態 $s$ から実行できるとは、FSM  $M$ が状態 $s$ であるときに、 $\alpha$ の入力系列 $i_1 i_2 \cdots i_m$ を $M$ に与えて得られる出力系列が $\alpha$ の出力系列 $o_1 o_2 \cdots o_m$ と一致することをいう。

一般に任意のFSMの各状態に対してUIO系列が存在するとは限らない。ただし、実際の通信プロトコルでは、ほとんどの場合に各状態に対してUIO系列が存在することが知られている。また、各状態に対するUIO系列は複数個存在する場合がある。

各状態を識別するためには、各状態について一つのU I O系列を用意すれば十分である。例えば、F i g. 3の状態  $s_0$  に対するU I O系列は、 $(y/2) (x/1)$  と  $(x/2) (y/1)$  である。F i g. 3のF S Mの各状態  $s_i$  に対するU I O系列はF i g. 4に示す表のようになる。

各状態を識別するためには、各状態について1つのU I O系列があれば十分であるが、各状態に対して複数のU I O系列を用意して、それらのU I O系列から適切な系列を選ぶことによって、試験系列がより短くなる場合がある。

また、複数のU I O系列が重複部分を持つ場合、それらのU I O系列を重複させた系列を生成し、その系列を利用することでより短い試験系列を生成することができる場合がある。

#### (S A T問題)

S A T問題とは、与えられた和積形論理式  $f$  に対して充足可能性を判定し、充足可能であれば  $f$  中の変数に対する真理値割当を算出する問題である。論理式  $f$  は複数個の節の論理積で構成され、それぞれの節は変数  $x$ 、または変数の否定  $\neg x$  の論理和で構成される。

S A T問題に対して、数多くのアルゴリズムが研究・開発されている。これらのアルゴリズムはComplete型とIncomplete型に分類される。Complete型アルゴリズムは、論理式に対して充足可能となるすべての真理値割り当てを算出することができ、解の存在の有無を決定することができる。

しかし、この型の多くのアルゴリズムは解空間のすべてを探索するために、大規模な問題を解くことが困難である。この型のアルゴリズムとしてG R A S P、S A T Zなどがある。

一方Incomplete型アルゴリズムは、与えられた問題に対する解の存在の有無は決定できないが、充足可能な場合に充足可能となる一つの真理値割り当てを高速に算出する場合があるアルゴリズムである。

つまり、解空間の一部分を抽出し探索空間を減らすことで、高速に解を算出する方法である。このためComplete型では解くことが難しい大規模問題に対しても解を算出することができる。この型のアルゴリズムとしてMIPS\_\_SAT、DLMなどがある。

プロトコル機械の各状態に対してUIO系列が存在する場合、そのプロトコル機械に対する試験系列は必ず存在するので、本発明ではIncomplete型アルゴリズムを使用する。DIMACSベンチマークテストの結果からMIPS\_\_SATを使用することにした。以降、SATアルゴリズムの実装をSATsolverと呼ぶ。

Fig. 5は、本発明の実施例1に係る試験系列生成処理フローの例を示す図である。本発明の実施例1における試験系列生成装置1は、以下のステップS1からステップS3を実行することによりプロトコル機械の各状態が正しく実装されているかを確認する試験系列を生成する。

ステップS1：プロトコルの仕様を示すFSM M、Mの各状態に対するUIO系列、確認したい状態、最大試験系列長を入力する。このステップS1は、仕様入力部11により実行される。

ステップS2：試験系列生成問題をSAT問題へ変換する。このステップS2は、試験系列生成問題変換部12により実行される。

ステップS3：既存のSATsolver（例えば、MIPS\_\_SAT）を用いて、SAT問題を解いて、試験系列を生成する。このステップS3は、試験系列生成部13により実行される。

本発明の実施例1では、プロトコル仕様を表すFSM MとMの各状態に対するUIO系列から和積形論理式を生成し、その論理式をSATsolverを用いて解くことで試験系列を生成する。

本発明の実施例1の提案手法では、各状態に対して論理変数を割当てて。まず、UIO系列に対応する状態とその状態に関連する状態遷移をMに追加してM'を生成する（FSMの修正）。その後M'の動作および試験系列に対する条件を表した論理式を構成する。



すなわち、上記ステップS 2 の、試験系列生成問題をSAT問題に変換するステップは、FSM修正部1 2 1がFSMを修正するステップと、和積形論理式定式化部1 2 2が修正後のFSMに基づいて試験系列生成問題を和積形論理式の節で表現するステップとから構成される。

まず、FSMを修正するステップについて説明する。FSM  $M = (S, X, Y, H, s_0)$  にUIO系列に対応する状態および関連する状態遷移を追加してFSM  $M' = (S \cup S', X, Y, H \cup H', \{s_0\} \cup I')$  を生成する。

$S'$  は新しく追加する状態の集合で、UIO系列1つに対して状態を1つ追加する。状態  $s_i$  に対するUIO系列で、UIO系列を状態  $s_i$  で実行すると状態  $s_j$  へ遷移するとき、状態  $s_{ij}$  を追加する。

上記のUIO系列に対応する状態とは、確認したい状態に対するUIO系列の始状態の入力遷移と同じ入力遷移を持ち、かつ、確認したい状態に対するUIO系列の終状態の出力遷移と同じ出力遷移を持つ状態のことをいう。

例えば、Fig. 3のFSMと状態  $s_0$  に対するUIO系列  $(y/2) (x/1)$  に対して後述する図7に示すように状態  $s_{00}$  を追加する。この状態は  $s_0 \rightarrow s_3 \rightarrow s_0$  を表している。確認したい状態  $s_0$  に対するUIO系列  $(y/2) (x/1)$  の始状態  $s_0$  の入力遷移は、 $s_3 \rightarrow s_0$  と  $s_1 \rightarrow s_0$  であるため、追加する状態  $s_{00}$  の入力遷移は  $s_3 \rightarrow s_{00}$  と  $s_1 \rightarrow s_{00}$  である。

また、確認したい状態  $s_0$  に対するUIO系列  $(y/2) (x/1)$  の終状態  $s_0$  の出力遷移は、 $s_0 \rightarrow s_4$  と  $s_0 \rightarrow s_3$  であるため、追加する状態  $s_{00}$  の出力遷移は、 $s_{00} \rightarrow s_4$  と  $s_{00} \rightarrow s_3$  である。また、UIO系列  $(x/2) (y/1)$  に対しては、上記基準に従って状態  $s_{01}$  を追加する。

$H'$  は  $s' \in S'$  に関係する遷移を表し、 $I' \subseteq S'$  は  $S'$  の要素のうち初期状態となり得る状態の集合を表している。例えばFig. 6に示すアルゴリズムに示すように  $H'$

、 $I'$  を構成する。状態  $s_{ij}$  への遷移は状態  $s_i$  への遷移、状態  $s_{ij}$  からの遷移は状態  $s_j$  からの遷移と同じものにする。

Fig. 3のFSMに状態  $s_{00}$ 、 $s_{01}$ と関係する状態遷移を加えるとFig. 7のようになる。図中の破線矢印が追加した状態遷移である。また、状態  $s_{00}$ 、 $s_{01}$ は $I'$ の要素である。

次に、UIO系列が重複部分を持つ場合、重複させた系列に対する状態を追加する。例えば、状態  $s_3$  に対するUIO系列  $(y/1) (y/1)$  と状態  $s_4$  に対するUIO系列  $(x/1) (y/1)$  を重複させて系列  $(x/1) (y/1) (y/1)$  を生成し、これに対応する状態としてここでは図示していない状態  $s_{41}$  を用意する。関係する状態遷移は上述した基準に従って生成する。

この構成法ではFSMの構造によって追加した状態間の遷移が生成されないことがある。Fig. 8AのFSMが通信プロトコルの仕様であり、遷移  $a$  が状態  $s_1$  のUIO系列、遷移  $b$  が状態  $s_2$  のUIO系列であるとする。上述した基準に従ってFig. 8AのFSMに新しい状態と状態遷移を追加すると、Fig. 8Bとなる。

このFSMでは、追加した状態（UIO系列）を連続して通過することができず、最短の試験系列が生成できない。そこで、自己ループを持たない状態に対してFig. 9Aのようにループ遷移を追加する（図中の遷移  $c$ 、 $d$ ）。ループを追加しておき、Fig. 9AのFSMを修正することによりFig. 9BのようなFSMが生成される。生成した試験系列に追加したループ遷移が含まれているときは、これを削除する。

次に、修正後のFSMに基づいて試験系列生成問題を和積形論理式の節で表現するステップについて説明する。本発明の実施例1の提案手法では、FSMは時刻0から動作を開始し、1単位時間ごとに遷移を1つ実行するものとする。

論理変数  $X[t][i]$  を用いて和積形論理式を作成する。 $X[t][i]$  が真の場合、時刻  $t$  でFSMが状態  $s_i$  であることを表す。例えば、Fig. 3のFSMに対して3単位時間の動作を考える。このときの動作を表すには  $X[t][i] (0 \leq t \leq 2, 0 \leq$

$i \leq 4$ ) の変数が必要である。

F S Mが状態  $s_0, s_4, s_1$  の順に遷移することを表すには、 $X[0][0]$ 、 $X[1][4]$ 、 $X[2][1]$  を真、これら以外の変数を偽とすればよい。

上記導入した論理変数を用いて、F S M  $M'$  の動作を表す論理式、および試験系列に対する条件を表す論理式を構成する。本発明の実施例1の提案手法では論理式を構成するために最大試験系列長（時刻の最大値） $T$ を与える。

（初期状態に対する条件）

$M'$  の初期状態は  $s_0 \cup I'$  である。そこで、時刻0では、 $M'$  は  $s_0 \cup I'$  のいずれか1つの状態であることを表す論理式を構成する。

F i g. 7のF S Mでは状態  $s_0, s_{00}, s_{01}$ がこの集合に含まれるので以下のようになる。

$$\begin{aligned} & (X[0][0] \vee X[0][00] \vee X[0][01]) \\ & \wedge (\neg X[0][0] \vee \neg X[0][00]) \\ & \wedge (\neg X[0][00] \vee \neg X[0][01]) \\ & \wedge (\neg X[0][0] \vee \neg X[0][01]) \end{aligned} \quad (式1)$$

（各時刻での状態に対する条件）

時刻0以外の各時刻において、F S Mは  $S \cup S'$  のうち1つの状態であることを示す論理式を構成する。F i g. 7のF S Mでは、以下のようになる。

$$\begin{aligned} & (X[t][0] \vee X[t][1] \cdots \vee X[t][44]) \\ & \wedge (\neg X[t][0] \vee \neg X[t][1]) \cdots \\ & \wedge (\neg X[t][1] \vee \neg X[t][44]) \quad (1 \leq t \leq T) \end{aligned} \quad (式2)$$

F S Mには、初期状態から一遷移（一単位時間）で到達できない状態がある。そこで、これらの状態を考慮することで、論理式のサイズを小さくすることができる。

（状態遷移を表す条件）

ある時刻  $t$  での状態が決定すれば、次の時刻に遷移することができる状態が決まる。こ

のことから、状態遷移を“状態→遷移可能なすべての状態の論理和”で表現することができる。

F i g. 7の状態 $s_4$ からは、状態 $s_1$ 、または $s_3$ へ遷移することができるので、以下ようになる。

$$X[t][4] \rightarrow (X[t+1][1] \vee X[t+1][3]) \quad (0 \leq t \leq T-1) \quad (\text{式 3})$$

(U I O系列を通過する条件)

0からTのいずれかの時刻で、各U I O系列(状態 $s' \in S'$ )を通過することを表す論理式を構成する。F i g. 7のF S Mに対してここでは図示していない $s_{22}$ を追加したとすると次のようになる。

$$(X[0][22] \vee X[1][22] \vee \cdots \vee X[T][22]) \quad (\text{式 4})$$

ある状態に対して複数のU I O系列がある場合は、それらのいずれかを通過することを表す論理式を構成する。状態 $s_0$ のU I O系列に対して状態 $s_{00}$ 、 $s_{01}$ を追加したとすると次のようになる。

$$(X[0][00] \vee X[1][00] \vee \cdots \vee X[T][00]) \vee (X[0][01] \vee X[1][01] \vee \cdots \vee X[T][01]) \quad (\text{式 5})$$

また、重複させたU I O系列については、重複させる前のU I O系列または重複させた後のU I O系列のいずれかを通ることを表す論理式を構成する。例えば状態 $s_3$ のU I O系列に対してここでは図示していない状態 $s_{31}$ 、状態 $s_4$ のU I O系列に対して図示していない $s_{44}$ 、重複させたU I O系列に対して図示していない $s_{41}$ をそれぞれ追加したとすると次のようになる。

$$\begin{aligned} & \{ (X[0][31] \vee \cdots \vee X[T][31]) \\ & \vee (X[0][41] \vee \cdots \vee X[T][41]) \} \wedge \\ & \{ (X[0][44] \vee \cdots \vee X[T][44]) \\ & \vee (X[0][41] \vee \cdots \vee X[T][41]) \} \end{aligned} \quad (\text{式 6})$$

以上の条件を表す論理式は、それぞれ簡単に和積形に整理することができる。和積形に整理した(式1)～(式6)までの論理式の論理積をとることによって得られる論理式が、試験系列生成問題に対応する和積形論理式である。

そして、上記ステップS3において、この論理式をSAT solverに適用して解を求め、各時刻でのFSMの状態を得る。UIO系列に対応する状態はその状態が表す状態と状態遷移に展開した後、遷移だけを取り出すことで、試験系列が得られる。例えば、Fig. 7に示すFSMにおいて、UIO系列に対応する状態 $s_0$ については、 $s_0 \rightarrow s_3 \rightarrow s_0$ に展開した後、遷移を取り出して、試験系列を得る。

本発明の実施例1の提案手法では、問題の入力として最大試験系列長Tを与える。状態の存在確認を行う試験系列では、各状態に対して、その状態を識別するUIO系列を1回以上通る必要があるため、Tの値として、状態の数よりも大きな値を与える必要がある。値が小さいことによって解が得られない場合は、より大きな値を与えて論理式を構成する。

次に、本発明の実施例1の試験系列生成方法をFig. 3に示すFSMとFig. 10に示すDHCPの動作を示すFSMに対して適用した。

まず、Fig. 3のFSMで表されるプロトコルに対して、試験系列を生成した。試験系列を生成するための論理式に含まれる変数の数、節の数および生成された試験系列の長さをFig. 11に示す。

実験1は、各状態のUIO系列が1で重複を考慮しない場合、実験2は、各状態のUIO系列数が複数で重複を考慮しない場合、実験3は、各状態のUIO系列が1で重複を考慮する場合、実験4は、各状態のUIO系列数が複数で重複を考慮する場合である。

UIO系列の重複を考慮した方が、より短い試験系列が生成されている。また、この例では状態 $s_0$ に対して2つのUIO系列を用意しても生成される試験系列の長さは変わらなかった。

次に、Fig. 10に示すDHCPに対する適用結果について説明する。DHCPのク

クライアント側プロトコルに対して試験系列を生成した。DHCPとは、ネットワーク上のクライアントにサーバを利用してIPアドレスを動的に割り当てるプロトコルである。DHCPを表すFSMの状態数は14、状態遷移数は77である。

DHCPに対して、各状態に対するUIO系列を作成した。UIO系列が1つの状態が10、UIO系列が2つの状態が4であった。試験系列生成問題を論理式に変換し、SATsolverに適用して試験系列を求めた。得られた試験系列の長さは21であった。

生成した論理式の変数の数、節の数、生成時間およびSATsolverの実行時間は、Fig. 12の1行目のようになった。各時間は5回の平均（秒）で、実行環境はCPU PentiumIII 700MHz、メモリ1GBである。

また、実験のために各状態に対して複数の系列を割り当て、そのいずれかを含む系列を生成した。結果を、Fig. 12の表の2から4行目に示す。2行目は、各状態に1本、3行目は2本、4行目は3本の系列を割り当てた結果である。

上述のように、本発明の実施例1では、FSM通信プロトコルに対して、状態確認を行うための試験系列をSATを用いて生成する手法を提案した。提案手法では、各状態に複数のUIO系列がある場合、およびUIO系列の重複を考慮して最適な試験系列を生成することができることがわかる。そして、DHCPに対して提案手法を適用し試験系列が生成できることを確認した。

#### （実施例2）

本発明の実施例2では、部分系列を利用して、プロトコル仕様に記述されている状態遷移が正しく実装されているかを試験する試験系列を生成する。具体的には、本発明の実施例2では、SATアルゴリズムを用いて、従来手法では困難であった部分系列の重複を考慮した効率的な試験系列を生成する手法を提案する。

本発明の実施例2においても、本発明の実施例1と同様に、SAT問題を解くためにSATsolverとしてMIPS\_\_SATを使用する。

次に、適合性試験について説明する。通信プロトコルの仕様をモデル化したMealy

型FSMの例をFig. 13に示す。ここでFSMの各状態はプロトコルのある状態に対応し、各状態遷移はプロトコルの動作に対応している。

仕様に基づいた実装（IUT：Implementation Under Test）に対して、各動作が正しく実装されているかどうかを試験する必要がある（適合性試験）。例えば遷移 $s_2 \rightarrow s_5$ に対する試験は以下のようにして行う。

1. IUTを初期状態から状態 $s_2$ へ遷移させる。
2. 入力 $a$ を与え、出力 $w$ が得られるかを確認する。
3. 次に、IUTが状態 $s_5$ に遷移したかどうかを確認する。 $s_5$ に遷移したことが確認された場合、その遷移が正しく実装されていると判断する。

上記の方法ですべての状態遷移に対して試験を行い、IUTが仕様を満たしているかどうかを判断する。そのためFSMの各状態を識別する方法が重要となる。

FSMの各状態を識別する方法として、実施例1において説明したUIO系列を用いた方法がある。例えば、Fig. 13のFSMの各状態に対するUIO系列はFig. 14に示す表のようになる。

UIO系列を使用すると、ある遷移と遷移先状態のUIO系列による遷移系列を接続した遷移系列によって遷移が正しく実装されているかどうかを確認することができる。以後、ある遷移 $e$ と $e$ の遷移先状態のUIO系列による遷移系列を接続した遷移系列を“部分系列”と呼び、 $seq(e)$ と記述する。

次に、本発明の実施例2における試験系列生成問題の定義を行う。

(入力)

- ・プロトコル仕様を表す FSM  $M$
- ・ $M$ の各状態に対するUIO系列
- ・試験したい状態遷移の集合 $E = \{e_1, e_2, \dots, e_n\}$
- ・順序制約、時間制約
- ・最大試験系列長 $T$

(出力)

- ・ 試験系列

(制約条件)

- ・ 試験系列は初期状態から始まる。
- ・ 試験系列はEに対応する部分系列  $\{seq(e_i) \mid e_i \in E\}$  をすべて含む。

(目的条件)

- ・ 試験系列長の最短化

順序制約とは、各遷移を実行する順序に対する制約である。また、時間制約とは、ある遷移は別の遷移を実行した後一定時間のみ実行可能となるような遷移の実行時間に対する制約である。

従来から、FSMの各状態が自己ループを持つ、または各状態から初期状態への遷移（リセット遷移）が存在する場合に、試験系列生成問題を多項式時間で解く手法が提案されている。しかし、部分系列を重ね合わせを考慮した効率の良い試験系列生成手法は提案されていない。本発明の実施例2では、部分系列の重ね合わせを考慮した効率の良い試験系列生成を行う。

本発明の実施例2では、以下のようにして試験系列を生成する。Fig. 15は、本発明の実施例2に係る試験系列生成処理フローの例を示す図である。

ステップS11：プロトコルの仕様を示すFSM M、Mの各状態に対するUIO系列、試験したい状態遷移、順序制約、時間制約、最大試験系列長を入力する。このステップS11は、仕様入力部11により実行される。

ステップS12：試験系列生成問題をSAT問題へ変換する。このステップS12は、試験系列生成問題変換部12により実行される。

ステップS13：既存のSAT solver（例えばMIPS\_\_SAT）を用いて、SAT問題を解いて、試験系列を生成する。このステップS13は、試験系列生成部13により実行される。



上記ステップS 1 2において示す、試験系列生成問題をSAT問題に変換するステップは、FSM修正部1 2 1がFSMを修正するステップと、和積形論理式定式化部1 2 2が修正後のFSMに基づいて試験系列生成問題を和積形論理式の節で表現するステップとから構成される。

また、本発明の実施例2においても、実施例1と同様に、和積形論理式を構成する論理変数として $X[t][i]$ を準備する。 $X[t][i]$ はある時刻 $t$ でFSMが状態 $s_i$ であるか否かを表す変数である。 $X[t][i]$ が真の場合、時刻 $t$ でFSMが状態 $s_i$ であることを表す。なおFSMは1単位時間ごとに遷移を1つ実行するものとする。

まず、FSMを修正するステップについて説明する。本発明の実施例2では、効率的な試験系列を生成するために、入力として与えられるFSMを次のように修正する。

(終状態におけるFSMの修正)

通常は、入力した最大試験系列長 $T$ よりも短い系列で終状態に到達する。このため与えられたFSMの終状態に入力dummyに対して、出力nullを返す自己ループを追加する。これにより、長さ $T$ 以下の試験系列を生成することができる。一方、入力した系列長が短く、解が存在しない場合には、より長い系列長を入力して試験系列を生成する。

(部分系列によるFSMの修正)

試験系列生成問題をSAT問題へ変換する際、部分系列を必ず通過する系列を探索できるようにするため、試験したい状態遷移に対する部分系列に相当する新しい状態をFSMに追加する。

試験したい状態遷移に対する部分系列に相当する新しい状態とは、試験したい遷移が必ず通過する部分系列の始状態の入力遷移と同じ入力遷移を持ち、この部分系列の終状態の出力遷移と同じ出力遷移を持つ状態をいう。

Fig. 13で表されるFSMと試験したい状態遷移 $A: s_2 \rightarrow s_5$ 、状態遷移 $B: s_1 \rightarrow s_2$ が存在する場合を考える。状態遷移 $A$ は部分系列 $seq(A): s_2 \rightarrow s_5 \rightarrow s_6$ を用いて試験することができることから、 $seq(A)$ を表す新しい状態( $s_{2,1}$ とする

）をFSMへ追加する。Fig. 16に示すように、この状態 $s_{21}$ は部分系列seq（A）の始状態 $s_2$ の入力遷移 $s_1 \rightarrow s_2$ 、 $s_3 \rightarrow s_2$ と同じ入力遷移 $s_1 \rightarrow s_{21}$ 、 $s_3 \rightarrow s_{21}$ を持ち、部分系列seq（A）の終状態 $s_6$ の出力遷移 $s_6 \rightarrow s_4$ と同じ出力遷移 $s_{21} \rightarrow s_4$ を持つようにする。

同様にして部分系列seq（B）： $s_1 \rightarrow s_2 \rightarrow s_5$ に相当する状態（ $s_{22}$ とする）と対応する遷移をFig. 16に示すように追加する。このように修正されたFSMにおける試験系列生成問題とは、初期状態 $s_1$ から始まり、状態 $s_{21}$ 、状態 $s_{22}$ を通り、終状態 $s_1$ へ至る系列を求める問題となる。そして生成された試験系列の状態 $s_{21}$ 、 $s_{22}$ をそれぞれ元の部分系列seq（A）、seq（B）と置き換えることにより試験系列が生成される。

（重複部分をもつ部分系列の合成）

効率的な適合性試験を行うためには、より系列長の短い試験系列の生成が重要である。そこで部分系列の重複部分を考慮した試験系列の生成について考察する。上述した例を使って説明する。2つの部分系列seq（A）、seq（B）には重複部分 $s_2 \rightarrow s_5$ が存在する。

この場合、状態 $s_{21}$ 、 $s_{22}$ で表される部分系列seq（A）、seq（B）をそれぞれ別々に通過する試験系列を生成するよりも、部分系列seq（A）、seq（B）の重複部分を考慮した新しい部分系列seq（A、B）（ $s_1 \rightarrow s_2 \rightarrow s_5 \rightarrow s_6$ ）を通過する系列を生成した方が試験系列長が短くなる場合がある。

本発明の実施例2の提案手法では、FSMに重複を考慮した部分系列を表す新しい状態を追加する。そして、後述する試験系列生成問題を和積形論理式の節で表現するステップにおいて、状態遷移Aに対してはseq（A）かseq（A、B）のいずれかを通過するための条件式を構成する。

具体的には、部分系列seq（A）、seq（B）の重複を考慮した部分系列seq（A、B）を表す新しい状態 $s_{23}$ を追加したFSM（Fig. 16）を作成する。そして、

後述する試験系列生成問題を和積形論理式の節で表現するステップにおいて、 $s_{21}$ か $s_{23}$ のいずれかを通過するための条件節を構成する。

次に、修正後のFSMに基づいて試験系列生成問題を和積形論理式の節で表現するステップについてFig. 16を用いて説明する。本発明の実施例2の提案手法では、まずFSMにおける試験系列生成問題を以下に述べる7つの制約条件に変換する。次に各制約条件を和積形論理式の節で表現し、SAT solverに適用することにより、試験系列を生成する。

条件1：初期状態から出発する制約

Fig. 16で初期状態は $s_1$ である。また部分系列Seq(B)の先頭の状態も $s_1$ である。そこで条件1では、初期状態を表す状態( $s_1$ 、 $s_{22}$ 、 $s_{23}$ )のいずれかが選択されることを表す節と、同時に2つ以上の状態が選択されないことを表す節、の論理積を制約として与える。

$$\begin{aligned} & (X[0][0] \vee X[0][22] \vee X[0][23]) \\ & \wedge (\neg X[0][1] \vee \neg X[0][22]) \\ & \wedge (\neg X[0][1] \vee \neg X[0][23]) \\ & \wedge (\neg X[0][22] \vee \neg X[0][23]) \quad (\text{式7}) \end{aligned}$$

条件2：時刻Tに終状態で終了する制約

Fig. 16では $s_1$ のみが終状態である。ただし、ある部分系列の最後の状態が $s_1$ である場合は、その部分系列を表す状態も終状態とみなし、条件1と同様の制約を与える。Fig. 16の場合、以下ようになる。

$$X[T][1] \quad (\text{式8})$$

条件3：各時刻で状態を1つ選択する制約

Fig. 16のFSM上のすべての状態から、各時刻で1つの状態が選択される制約条件である。状態 $s_1 \sim s_{23}$ のうちいずれかの状態が選択されることを表す節と、同時に2つ以上の状態が選択されないことを表す節、の論理積で表される。

$$\begin{aligned}
& (X[t][1] \vee X[t][2] \vee X[t][3] \vee \dots X[t][23]) \\
& \wedge (\neg X[t][1] \vee \neg X[t][2]) \\
& \wedge (\neg X[t][1] \vee \neg X[t][3]) \dots \\
& \wedge (\neg X[t][22] \vee \neg X[t][23]) \quad (0 < t < T) \quad (\text{式9})
\end{aligned}$$

ここでFSM上の各状態は初期状態からある一定の時間が経過した後到達可能となる。同様に各状態から終状態への遷移も、ある一定遷移時間が経過した後、到達可能となる。各状態の到達可能時刻を考慮することで、節数を削減することができる。

具体的にFig. 16では、初期状態から一遷移で到達可能な状態は $s_{22}$ 、 $s_{23}$ を除いた7つの状態である。そこで(式9)を、これらの状態で構成することにより節数が少なくなる。

条件4：各状態の各時刻での状態遷移を表す制約

FSMの状態遷移は、“状態 $\wedge$ 入力 $\rightarrow$ 次状態”で表現される。しかし、上記条件1、3により、これを“状態 $\rightarrow$ 遷移可能なすべての状態の論理和”で表現できる。例えばFig. 16の状態 $s_2$ からは、状態 $s_3$ 、 $s_5$ へ遷移できるので、以下のようになる。

$$\begin{aligned}
& X[t][2] \rightarrow (X[t+1][3] \vee X[t+1][5]) \quad (0 \leq t \leq T-1) \\
& (\text{式10})
\end{aligned}$$

条件5：部分系列を必ず通過する制約

最初から最後のいずれかの時刻で、各部分系列を必ず通過することを表す制約条件である。これは部分系列を表す追加された状態(Fig. 16では状態 $s_{21}$ 、 $s_{22}$ )を必ず通過することを表す制約式により表現される。

$$\begin{aligned}
& (X[0][21] \vee X[1][21] \vee \dots \vee X[T][21]) \\
& \wedge (X[0][22] \vee X[1][22] \vee \dots \vee X[T][22]) \quad (\text{式11})
\end{aligned}$$

なお、Fig. 16のように重複部分を持つ部分系列が存在する場合、状態遷移Aに対しては $s_{21}$ 、 $s_{23}$ のいずれか一方(状態遷移Bに対しては $s_{22}$ 、 $s_{23}$ のいずれが一方)を通過すればよいので、以下の制約式を与える。

$$\begin{aligned}
& \{ (X[0][21] \vee X[1][21] \vee \cdots \vee X[T][21]) \\
& \vee (X[0][23] \vee X[1][23] \vee \cdots \vee X[T][23]) \} \wedge \\
& \{ (X[0][22] \vee X[1][22] \vee \cdots \vee X[T][22]) \\
& \vee (X[0][23] \vee X[1][23] \vee \cdots \vee X[T][23]) \} \quad (\text{式12})
\end{aligned}$$

条件6：順序制約を表す制約

順序制約とは、複数の遷移間における実行順序に関する制約である。例えば、Fig. 16の2つの部分系列seq(A)、seq(B)の間に、部分系列seq(B)を実行するにはそれ以前に部分系列seq(A)が実行されていなければならないという順序制約が存在する場合、以下のようになる。

$$\begin{aligned}
& \{ (X[t][21] \rightarrow X[t+1][22] \vee X[t+2][22] \vee \cdots \vee X[T][22]) \} \\
& \wedge \{ X[t][21] \rightarrow \\
& (\neg X[t-1][22] \vee \neg X[t-2][22] \vee \cdots \vee \neg X[0][22]) \} \\
& (0 \leq t \leq T-1) \quad (\text{式13})
\end{aligned}$$

条件7：時間制約を表す制約

時間制約とは、初期状態から一定時間以内にある遷移を実行しなければならない、あるいはある遷移を実行したあと一定時間以内に遷移を実行しなければならないなど、遷移の実行時間に対する制約である。

例として、部分系列seq(A)が $(0 \leq t \leq 10)$ の条件で実行されなければならない場合の表現方法を以下に示す。

$$X[0][21] \vee X[1][21] \vee \cdots \vee X[10][21] \quad (\text{式14})$$

上記の7つの制約条件で作成された条件節の論理積を取ることにより得られる論理式が、試験系列生成問題に対応する和積形論理式である。これをSAT solverに適用し、解を求めることにより、試験系列が生成される。

提案手法では、問題の入力として最大試験系列長Tを与える。試験系列では部分系列に

対応する状態を必ず通過する必要があるので、Tの初期値として、部分系列よりも大きな値を与える必要がある。

#### (DHCPへの適用)

本発明の実施例2の試験系列生成方法を、Fig. 10に示すDHCPの動作を示すFSMに対して適用した。FSMの状態数は14、状態遷移数は77である。

#### (動作の制約条件がない場合の実行結果)

DHCPに対して、各状態のUIO系列を作成し、試験したい状態遷移の数を変化させて試験系列を生成した。指定した状態遷移数は30、45、60、70および77である。結果をFig. 17に示す。

系列長の括弧内の数字は、部分系列を表す状態を元の状態遷移に戻したあとの系列長である。実行時間は5回の平均(秒)で、実行環境はCPU Pentium III 700MHz、メモリ1GBである。この結果、提案手法はDHCPに対する試験系列を実用的時間で生成できることを確認した。

#### (順序制約・時間制約がある場合の実行結果)

試験系列生成問題に順序制約、時間制約が存在する場合について評価を行なった。例として、順序制約を2つ、時間制約を2つ設定した結果をFig. 18に示す。結果より、制約が存在しない場合と比較して節の数が増加しているが、制約が存在する場合も制約が存在しない場合とほぼ同等の計算時間で試験系列が生成できることを確認した。

#### (部分系列の重複を考慮した実行結果)

部分系列の重複を考慮した試験系列の生成についても評価を行なった。DHCPでは、2つの部分系列が重複する組合せが14組、3つの部分系列が重複する組合せが3組存在する。そこで、2つの部分系列が重複する組合せを考慮する条件を条件1、3つの部分系列が重複する組合せを考慮する条件を条件2とし、それぞれの条件を考慮した場合の試験系列を生成した結果をFig. 19に示す。

重複条件が存在しない場合の系列長91(342)に対し、条件1を考慮した場合は7

4 (3 2 1)、条件1、2の両方を考慮した場合は7 1 (3 1 3)であるので、より短い試験系列が生成された。実行時間においても、重複条件が存在しない場合に比べ、短い時間で試験系列が生成された。以上より、本発明の実施例2の提案手法は部分系列の重複を考慮した場合にも有用である。

(従来手法との比較)

F S Mの各状態が自己ループを持つ、または各状態から初期状態への遷移（リセット遷移）が存在する場合に、試験系列生成問題を多項式時間で解く従来手法を用いて、DHCPに対してすべての状態遷移を確認する試験系列を生成した。ここでは、特に部分系列の重複を考慮して試験系列を生成した。

上述したように、DHCPに対しては2つの部分系列が重複する組合せが14組ある。このとき、各組に対して元の系列を用いる場合および重ね合わせた系列を用いる場合の2通りがあるので、部分系列の組合せとしては $2^{14}$ 通りある。

問題によってはどちらの系列を用いるべきかを判定することができる場合もあるが、一般に上記従来手法を用いて最適な試験系列を求めるときには、部分系列の組合せを指定し、問題を $2^{14}$ 回解く必要があり、 $0.14 \times 2^{14} = 2293.76$ 秒程度の時間がかかると考えられる。

一方、本発明の実施例2の提案手法ではFig. 19の2行目の結果から約262秒で試験系列を生成することができる。

(系列長と実行時間に対する考察)

本発明の実施例2の提案手法では、入力として最大試験系列長Tを与える。系列長の初期値として、試験系列が存在し、実用的な時間で解が得られる値を入力することが望ましい。

一般に系列長を長くした場合、解の数が増加するため、高速に解を算出することができる。しかし、同時に節と変数の数が増加する。一般にSAT問題では、節と変数の数が増加すると、解の算出時間も増加する傾向にある。そのため系列長が試験系列の生成時間に

対してどのように影響するかを調べた。例題として、重複条件 1 を考慮した試験系列生成問題を使用した。結果を Fig. 20 に示す。

系列長を長くした場合、節と変数の数は増加している。また、系列長が 76 および 80 では実行時間が短くなっているが、90 および 100 では長くなっている。以上より、この問題に対しては、系列長が 100 程度であれば解が得られ、生成時間も実用的である。

このとき、 $100 \div 77 = 1.29$  なので部分系列数の 1.29 倍の値が系列長の初期値として適当であると考えられる。また、幾つかの実験結果から部分系列数の 1.25 倍程度の値を系列長の初期値とすると、ほとんどの場合で解が得られ、生成時間も実用的であった。



## 特許請求の範囲

### 1. 通信プロトコルの試験系列生成方法であって、

前記通信プロトコルの仕様を示す有限状態機械（F S M）のデータを入力する仕様入力ステップと、

前記通信プロトコルの試験系列生成問題をS A T問題へ変換する試験系列生成問題変換ステップと、

前記S A T問題を解いて前記通信プロトコルの試験系列を生成する試験系列生成ステップとを有する

ことを特徴とする。

### 2. 請求項1に記載の通信プロトコルの試験系列生成方法において、

前記試験系列生成問題は、通信プロトコルの仕様に記述されている状態が前記有限状態機械の実装に存在するのかを確認するための試験系列を生成する問題である

ことを特徴とする。

### 3. 請求項1に記載の通信プロトコルの試験系列生成方法において、

前記試験系列生成問題は、通信プロトコルの仕様に記述されている状態遷移が前記有限状態機械の実装に正しく実装されているのかを試験するための試験系列を生成する問題である

ことを特徴とする。

### 4. 請求項1または請求項2または請求項3に記載の通信プロトコルの試験系列生成方法において、

前記試験系列生成問題変換ステップは、

前記F S Mを修正するステップと、

修正後のF S Mに基づいて試験系列生成問題を和積形論理式の節で表現するステップとを有する

ことを特徴とする。

5. 請求項2に記載の通信プロトコルの試験系列生成方法において、  
前記試験系列生成問題変換ステップは、  
前記F S Mを修正するステップと、  
修正後のF S Mに基づいて試験系列生成問題を和積形論理式の節で表現するステップと  
を有し、

前記F S Mを修正するステップは、前記F S Mに前記F S Mの存在を確認したい各状態  
のU I O系列に対応する状態および関連する状態遷移を追加する  
ことを特徴とする。

6. 請求項5に記載の通信プロトコルの試験系列生成方法において、  
前記F S Mの存在を確認したい各状態のU I O系列に対応する状態は、  
存在を確認したい各状態に対するU I O系列の始状態の入力遷移と同じ入力遷移を持ち  
、かつ、存在を確認したい各状態に対するU I O系列の終状態の出力遷移と同じ出力遷移  
を持つ状態である  
ことを特徴とする。

7. 請求項3に記載の通信プロトコルの試験系列生成方法において、  
前記試験系列生成問題変換ステップは、  
前記F S Mを修正するステップと、  
修正後のF S Mに基づいて試験系列生成問題を和積形論理式の節で表現するステップと  
を有し、  
前記F S Mを修正するステップは、前記F S Mに試験したい状態遷移に対する部分系列  
に対応する状態を追加する  
ことを特徴とする。

8. 請求項7に記載の通信プロトコルの試験系列生成方法において、  
前記試験したい状態遷移に対する部分系列に対応する状態は、  
前記試験したい状態遷移が必ず通過する部分系列の始状態の入力遷移と同じ入力遷移を

持ち、この部分系列の終状態の出力遷移と同じ出力遷移を持つ状態である

ことを特徴とする。

9. 通信プロトコルの試験系列生成装置であつて、

前記通信プロトコルの仕様を示す有限状態機械（F S M）のデータを入力する仕様入力部と、

前記通信プロトコルの試験系列生成問題を S A T 問題へ変換する試験系列生成問題変換部と、

前記 S A T 問題を解いて前記通信プロトコルの試験系列を生成する試験系列生成部とを備える

ことを特徴とする。

10. 請求項9に記載の通信プロトコルの試験系列生成装置において、

前記試験系列生成問題は、通信プロトコルの仕様に記述されている状態が前記有限状態機械の実装に存在するのかを確認するための試験系列を生成する問題である

ことを特徴とする。

11. 請求項9に記載の通信プロトコルの試験系列生成装置において、

前記試験系列生成問題は、通信プロトコルの仕様に記述されている状態遷移が前記有限状態機械の実装に正しく実装されているのかを試験するための試験系列を生成する問題である

ことを特徴とする。

12. 請求項9または請求項10または請求項11に記載の通信プロトコルの試験系列生成装置において、

前記試験系列生成問題変換部は、

前記 F S M を修正する F S M 修正部と、

修正後の F S M に基づいて試験系列生成問題を和積形論理式の節で表現する和積形論理式定式化部とを備える

ことを特徴とする。

13. 請求項10に記載の通信プロトコルの試験系列生成装置において、

前記試験系列生成問題変換部は、

前記F SMを修正するF SM修正部と、

修正後のF SMに基づいて試験系列生成問題を和積形論理式の節で表現する和積形論理式定式化部とを備え

前記F SM修正部は、前記F SMに前記F SMの存在を確認したい各状態のU I O系列に対応する状態および関連する状態遷移を追加する

ことを特徴とする。

14. 請求項13に記載の通信プロトコルの試験系列生成装置において、

前記F SMの各状態のU I O系列に対応する状態は、

存在を確認したい各状態に対するU I O系列の始状態の入力遷移と同じ入力遷移を持ち、かつ、存在を確認したい各状態に対するU I O系列の終状態の出力遷移と同じ出力遷移を持つ状態である

ことを特徴とする。

15. 請求項11に記載の通信プロトコルの試験系列生成装置において、

前記試験系列生成問題変換部は、

前記F SMを修正するF SM修正部と、

修正後のF SMに基づいて試験系列生成問題を和積形論理式の節で表現する和積形論理式定式化部とを備え

前記F SM修正部は、前記F SMに試験したい状態遷移に対する部分系列に対応する状態を追加する

ことを特徴とする。

16. 請求項15に記載の通信プロトコルの試験系列生成装置において、

前記試験したい状態遷移に対する部分系列に対応する状態は、

前記試験したい状態遷移が必ず通過する部分系列の始状態の入力遷移と同じ入力遷移を持ち、この部分系列の終状態の出力遷移と同じ出力遷移を持つ状態であることを特徴とする。

## 開示の要約

本発明の通信プロトコルの試験系列生成方法および装置は、通信プロトコルの仕様を示す有限状態機械（FSM）のデータを入力し、前記通信プロトコルの試験系列生成問題をSAT問題へ変換し、前記SAT問題を解いて前記通信プロトコルの試験系列を生成する。

また、本発明は、前記試験系列生成問題をSAT問題へ変換する際に、前記FSMを修正し、修正後のFSMに基づいて試験系列生成問題を和積形論理式の節で表現する。

本発明によれば、複数のUIO系列およびUIO系列の重複を考慮して、プロトコル仕様に記述されている状態が前記有限状態機械の実装に存在するかを確認する最適な試験系列を生成することが可能となる。

また、本発明によれば、部分系列の重複を考慮して、プロトコル仕様に記述されている状態遷移が前記有限状態機械の実装に正しく実装されているかを試験する最適な試験系列を生成することが可能となる。